REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed December 8, 2006.

1. Response to Objection of Claims

Claim 1 has been amended to overcome the objection cited in the Office Action in one of the manners suggested by the Examiner. Therefore, withdrawal of the objection is respectfully requested.

2. Response to Rejection of Claims Under 35 U.S.C. §103(a)

In the Office Action, claims 1-12 and 14-19 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Linsker* (U.S. Patent No. 5,598,473) in view of *Mazzagatte* (U.S. Patent No. 6,862,583) in further view of *Davis* (U.S. Patent No. 5,633,932) in further view of *Menezes* (Handbook of Applied Cryptography). It is well-established at law that, for a proper rejection of a claim under 35 U.S.C. §103 as being obvious based upon a combination of references, the cited combination of references must disclose, teach, or suggest, either implicitly or explicitly, all elements/features/steps of the claim at issue. *See, e.g.*, *In Re Dow Chemical*, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1988), and *In re Keller*, 208 U.S.P.Q.2d 871, 881 (C.C.P.A. 1981).

a. Independent Claim 1

Applicants respectfully submit that independent claim 1 is allowable for at least the reason that *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* does not disclose, teach, or suggest at least "receiving

and securely retaining a digital document and a transmitted independently verifiable data record of the intended recipient at a printout station, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender" or "decoding encrypted identification data with the first token of the intended recipient, the encrypted identification data being identification data from the independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station," as recited in claim 1.

The Office Action cites *Mazzagatte* in support of disclosing the features directed at verifying the identity of an intended recipient of a document. However, *Mazzagatte* teaches that encryption and decryption operations are both performed at a print node. Further, *Mazzagatte* clearly explains that "the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node." Cols. 8-9, lines 62-1. Therefore, any encryption performed at a sending node is not performed for identification verification or authentication purposes. Thus, *Mazzagatte* fails to teach or show an "independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station," as recited in the claim. (Emphasis added).

Linkser is inadequate to remedy the deficiencies of *Mazzagate* for at least the reason that *Linkser* does not teach or suggest that information is encrypted using a token of an intended recipient and then transmitted. In contrast, *Linsker* teaches that information is encrypted using a token of a sender and then transmitted.

Menezes is inadequate to remedy the deficiencies of *Mazzagate* and *Linkser* for at least the reason that *Menezes* does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient.

In the Office Action, *Davis* is alleged to disclose that identification data is encrypted by a transmission station. Page 6. However, *Davis* clearly states that "a header 260 for the document is encrypted using the public key "PUK" 210 of the targeted printing node" and that the header may contain a public key of an intended recipient of the printed copy. *See* col. 4, lines 45-65. As such, this header information is not encrypted using a public key of an intended recipient. For example, *Davis* states that the "printing node 130 first decrypts the encrypted header 265 using PRK 211 [private key of the printing node]" and then stores the document in buffer memory until the intended recipient is determined to be present. Col. 5, lines 10-24.

Each of the aforementioned cited references fail to teach or suggest features alleged in the Office Action, such as an "independently verifiable data record that is encrypted using a second token of the recipient by a transmitting station," as recited in the claim. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 1. It is further noted that one cannot show obviousness based on a combination of references if claimed features are not disclosed by any of the individual references of the proposed combination.

For at least these reasons, claim 1 is not obvious under the proposed combination, and the rejection should be withdrawn.

b. Claims 2-8

Because independent claim 1 is allowable over the cited art of record, dependent claims 2-8 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that the dependent claims 2-8 contain all features/elements of independent claim 1. *See, e.g., In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988). Accordingly, the rejection to these claims should be withdrawn.

c. Independent Claim 9

Applicants respectfully submit that independent claim 9, as amended, is allowable for at least the reason that *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* does not disclose, teach, or suggest at least "encoding identification data of the intended recipient using the first token of the intended recipient" and "sending the encrypted digest, the digital document, the second token of the sender, and the encoded identification data to the recipient," as recited in claim 9.

The Office Action cites *Mazzagatte* in support of disclosing the features directed at verifying the identity of an intended recipient of a document. However, *Mazzagatte* teaches that encryption and decryption operations are both performed at a print node. Further, *Mazzagatte* clearly explains that "the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node." Cols. 8-9, lines 62-1. Therefore, any encryption performed at a sending node is not performed for identification verification or authentication purposes. Thus,

Mazzagatte fails to teach or show "encoding identification data of the intended recipient using the first token of the intended recipient" and "sending the encrypted digest, the digital document, the second token of the sender, and the encoded identification data to the recipient," as recited in the claim.

Linkser is inadequate to remedy the deficiencies of *Mazzagate* for at least the reason that *Linkser* does not teach or suggest that information is encrypted using a token of an intended recipient and then transmitted. In contrast, *Linsker* teaches that information is encrypted using a token of a sender and then transmitted.

Menezes is inadequate to remedy the deficiencies of *Mazzagate* and *Linkser* for at least the reason that *Menezes* does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient. Applicants respectfully submit that *Menezes* describes a challenge-response technique where a random number is encrypted and does not teach or suggest "encoding identification data of the intended recipient using the first token of the intended recipient," as recited in claim 9.

In the Office Action, *Davis* is alleged to disclose that identification data is encrypted by a transmission station. Page 6. However, *Davis* clearly states that "a header 260 for the document is encrypted using the public key "PUK" 210 of the targeted printing node" and that the header may contain a public key of an intended recipient of the printed copy. *See* col. 4, lines 45-65. As such, this header information is not encrypted using a public key of an intended recipient. For example, *Davis* states that the "printing node 130 first decrypts the encrypted header 265 using PRK 211 [private key of the printing

node]" and then stores the document in buffer memory until the intended recipient is determined to be present. Col. 5, lines 10-24.

Each of the aforementioned cited references fail to teach or suggest features alleged in the Office Action, such as "encoding identification data of the intended recipient using the first token of the intended recipient" and "sending the encrypted digest, the digital document, the second token of the sender, and the encoded identification data to the recipient," as recited in the claim. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 9. It is further noted that one cannot show obviousness based on a combination of references if claimed features are not disclosed by any of the individual references of the proposed combination.

For at least these reasons, claim 9 is not obvious under the proposed combination, and the rejection should be withdrawn.

d. Claims 10-12 and 14-17

Because independent claim 9 is allowable over the cited art of record, dependent claims 10-12 and 14-17 (which depend from independent claim 9) are allowable as a matter of law for at least the reason that the dependent claims 10-12 and 14-17 contain all features/elements of independent claim 9. Accordingly, the rejection to these claims should be withdrawn.

e. Independent Claim 18

Applicants respectfully submit that independent claim 18, as amended, is allowable for at least the reason that *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* does not disclose, teach, or suggest at least "a communications module arranged to receive an electronic version of the transmitted document over a communications network, an independently verifiable data record of the intended recipient, a first token of the intended recipient, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender, a second token relating to the first token of the sender, and encrypted identification data of the intended recipient, the encrypted identification data being encrypted using a first token of the intended recipient," as recited in claim 18.

Further, *Mazzagatte* teaches that encryption and decryption operations are both performed at a print node, and *Mazzagatte* clearly explains that "the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node." Cols. 8-9, lines 62-1. Therefore, any encryption performed at a sending node is not performed for identification verification or authentication purposes. Thus, *Mazzagatte* fails to teach or show "a communications module arranged to receive an electronic version of the transmitted document over a communications network, an independently verifiable data record of the intended recipient, a first token of the intended recipient, an encrypted digest of the document created by the sender using a hash algorithm, the digest

being encrypted using a first token of the sender, a second token relating to the first token of the sender, and encrypted identification data of the intended recipient, the encrypted identification data being encrypted using a first token of the intended recipient," as recited in the claim.

Linkser is inadequate to remedy the deficiencies of *Mazzagate* for at least the reason that *Linkser* does not teach or suggest that information is encrypted using a token of an intended recipient and then transmitted. In contrast, *Linsker* teaches that information is encrypted using a token of a sender and then transmitted.

Menezes is inadequate to remedy the deficiencies of *Mazzagate* and *Linkser* for at least the reason that *Menezes* does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient.

Applicants respectfully submit that *Menezes* describes a challenge-response technique where a random number is encrypted and does not teach or suggest "wherein the second token of the intended recipient is used to decode encrypted identification data of the intended recipient that is compared to contents of the independently verifiable data record of the intended recipient to determine authenticity of the intended recipient," as recited in claim 18.

In the Office Action, *Davis* is alleged to disclose that identification data is encrypted by a transmission station. Page 6. However, *Davis* clearly states that "a header 260 for the document is encrypted using the public key "PUK" 210 of the targeted printing node" and that the header may contain a public key of an intended recipient of the printed copy. *See* col. 4, lines 45-

65. As such, this header information is not encrypted using a public key of an intended recipient. For example, *Davis* states that the "printing node 130 first decrypts the encrypted header 265 using PRK 211 [private key of the printing node]" and then stores the document in buffer memory until the intended recipient is determined to be present. Col. 5, lines 10-24.

Each of the aforementioned cited references fail to teach or suggest features alleged in the Office Action, such as "wherein the second token of the intended recipient is used to decode encrypted identification data of the intended recipient that is compared to contents of the independently verifiable data record of the intended recipient to determine authenticity of the intended recipient," as recited in the claim. Other references in the proposed combination fail to remedy the deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 18. It is further noted that one cannot show obviousness based on a combination of references if claimed features are not disclosed by any of the individual references of the proposed combination.

For at least these reasons, claim 18 is not obvious under the proposed combination, and the rejection should be withdrawn.

f. Independent Claim 19

Applicants respectfully submit that independent claim 19, as amended, is allowable for at least the reason that *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* does not disclose, teach, or suggest at least "a controller arranged to create a digest of the document using a hash algorithm and to encrypt the digest using a first token of the

sender and to encrypt identification data of the intended recipient using a first token of the intended recipient" and "a communications module arranged to obtain a second token of the sender related to the first token of the sender, which can be used to decrypt the encrypted digest and to send the encrypted digest, the digital document, the second token of the sender, the encrypted identification data of the intended recipient, and the first token of the intended recipient to the recipient," as recited in claim 19.

Further, *Mazzagatte* teaches that encryption and decryption operations are both performed at a print node, and *Mazzagatte* clearly explains that "the print node assumes that all data received via a secure transmission protocol, here SSL, is confidential and requires authentication before printout; and as a consequence the print job is encrypted and stored by the print node." Cols. 8-9, lines 62-1. Therefore, any encryption performed at a sending node is not performed for identification verification or authentication purposes. Thus, *Mazzagatte* fails to teach or show "a controller arranged to create a digest of the document using a hash algorithm and to encrypt the digest using a first token of the sender and to encrypt identification data of the intended recipient using a first token of the intended recipient" and "a communications module arranged to obtain a second token of the sender related to the first token of the sender, which can be used to decrypt the encrypted digest and to send the encrypted digest, the digital document, the second token of the sender, the encrypted identification data of the intended recipient, and the first token of the intended recipient to the recipient," as recited in the claim.

Linkser is inadequate to remedy the deficiencies of *Mazzagate* for at least the reason that *Linkser* does not teach or suggest that information is

encrypted using a token of an intended recipient and then sent to a recipient. In contrast, *Linsker* teaches that information is encrypted using a token of a sender and then transmitted.

Menezes is inadequate to remedy the deficiencies of *Mazzagate* and *Linkser* for at least the reason that *Menezes* does not teach or suggest using a token of an intended recipient to encrypt information that is transmitted by a sender to the recipient. Applicants respectfully submit that *Menezes* describes a challenge-response technique where a random number is encrypted and does not teach or suggest "to encrypt identification data of the intended recipient using a first token of the intended recipient," as recited in claim 19.

In the Office Action, *Davis* is alleged to disclose that identification data is encrypted by a transmission station. Page 6. However, *Davis* clearly states that "a header 260 for the document is encrypted using the public key "PUK" 210 of the targeted printing node" and that the header may contain a public key of an intended recipient of the printed copy. *See* col. 4, lines 45-65. As such, this header information is not encrypted using a public key of an intended recipient. For example, *Davis* states that the "printing node 130 first decrypts the encrypted header 265 using PRK 211 [private key of the printing node]" and then stores the document in buffer memory until the intended recipient is determined to be present. Col. 5, lines 10-24.

Each of the aforementioned cited references fail to teach or suggest features alleged in the Office Action, such as "to encrypt identification data of the intended recipient using a first token of the intended recipient," as recited in the claim. Other references in the proposed combination fail to remedy the

deficiencies of the individual references. Therefore, the proposed combination of references does not disclose all of the features of claim 19. It is further noted that one cannot show obviousness based on a combination of references if claimed features are not disclosed by any of the individual references of the proposed combination.

For at least these reasons, claim 19 is not obvious under the proposed combination, and the rejection should be withdrawn.

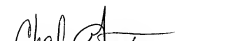
3. Response to Rejection of Claim Under 35 U.S.C. §103

Claim 13 was rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Linsker* in view of *Mazzagatte* in further view of *Davis* in further view of *Menezes* in further view of *Clark* (U.S. Patent 5,448,045). Because independent claim 9 is allowable over the cited art of record, dependent claim 13 (which depends from independent claim 9) is allowable as a matter of law for at least the reason that the dependent claim 13 contains all features/elements of independent claim 9 and *Clark* does not remedy the deficiencies of the *Linkser*, *Mazzagatte*, and *Menezes* references. Accordingly, the rejection to this claim should be withdrawn.

CONCLUSION

For at least the reasons set forth above, Applicants respectfully submit that all objections and/or rejections have been traversed, rendered moot, and/or accommodated, and that the pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned agent at (770) 933-9500.

Respectfully submitted,



Charles W. Griggers
Reg. No. 47,283